IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR SUPPRESSION OF EVIDENCE OBTAINED FROM GOOGLE ACCOUNT

The United States of America, by its undersigned attorneys, moves this Court to deny Defendant Okello T. Chatrie's motion to suppress evidence recovered from a search warrant for historical location information associated with his Google account for the period of May 1, 2019 through July 15, 2019. (ECF No. 20).

The defendant claims that the warrant is overbroad and fails to provide specific information about why the Google account would provide evidence other than location data. Neither of these contentions is accurate or supported by precedent, and the Court should reject the defendant's conclusory motion.

I. BACKGROUND[1]

At approximately 4:50 p.m. eastern standard standard time, on May 20, 2019, a then-unknown male entered the Call Federal Credit Union in Midlothian, Virginia with a firearm.

[1] The United States has provided defense counsel with full copies of all search warrant materials in this case. Their contention that redactions are made without explanation is belied by their failure to request such information. They are not entitled to the personal identifying information of others at this time.

While the man stood in line, victim-teller J.B. asked another teller, J.W., to assist this customer when he reached the counter. When he reached J.W.'s station, the man presented a handwritten note. That note read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt . . . I need at least 100k." After J.W. told him that she did not have access to that amount of money, the armed robber pulled out a silver and black handgun. Waving the firearm around, he then directed J.W., other Call Federal Credit Union employees, and customers to move to the center of the lobby and get on the floor. Once there, the armed robber led victims behind the teller counter and into a back room where the Credit Union's safe was located.

Once in the back room, he ordered everyone to their knees at gunpoint and demanded that the bank manager open the safe. The Credit Union manager, fearing for his life, obliged by opening the safe and handing over $195,000 in United States currency.

After the armed robbery, victims dialed 911 to request assistance. When law enforcement arrived, they reviewed surveillance video from the credit union and determined that the armed robber entered the credit union from an area behind a nearby church, held a cellular telephone to his ear when entering the credit union, and ran back towards the church after the robbery. An employee of that church explained to law enforcement that he saw a suspicious individual in a newer model, blue Buick sedan prior to the time of the robbery.

With this information in hand, law enforcement sought and obtained a state search warrant on June 14, 2019, for information pertaining to anonymized accounts in the custody and control

of Google, Inc., identifying Google IDs[2] that were within the vicinity of the Call Federal Credit Union and the nearby church just prior to, and right after, the armed robbery. This search warrant is commonly referred to as a "GeoFence" warrant.[3]

Based on returns of information for 19 anonymized accounts from Google on June 28, 2019, law enforcement identified several accounts of interest. The lead case agent recognized at the outset that one particular Google ID (hereinafter, the "Chatrie Account") was likely the device involved in the armed robbery because, among other things, the Chatrie Account: (1) was near the church prior to the robbery at the same time that the church witness recalled seeing the suspicious individual in the dark blue Buick sedan; (2) was inside the credit union at the time of the robbery; and (3) immediately left the area following the robbery from an area near the church.

Pursuant to the state GeoFence search warrant, on July 10, 2019, Google provided additional location information and history for nine of the original nineteen anonymized Google IDs to account for thirty minutes before and thirty minutes after the armed robbery.

Based on a review of this additional location information, law enforcement discovered that the Chatrie Account traveled to XXXX Mason Dale Drive following the armed robbery. Law enforcement assessed XXXX Mason Dale Drive and found that a utilities inquiry showed the defendant listed as a subscriber for the Mason Dale address. Further database searches revealed that Chatrie was born in Jamaica, had purchased a silver and black nine millimeter G2C Taurus

[2] The information gleaned from Google pursuant to this search warrant was entirely anonymized through all but one phase—the final phase—of the returns for the warrant. More specifically, Google merely provided information associated with a "Device ID" number. Google explains that "the Device ID is used only for distinguishing unique devices in a particular user's location history and cannot be mapped to an Android ID or an IMEI/MEID."

[3] The United States provides a fuller rundown of the GeoFence warrant in its response in opposition to the defendant's motion to suppress the evidence obtained from that warrant.

semiautomatic firearm from Bob Moates Sports Shop less than one month before the armed robbery, and owned a blue, 2010 Buick Lacrosse. Virginia Employment Commission records showed Chatrie's most recent employment as The Home Depot. The Home Depot shared with law enforcement that Chatrie provided them with a home address of XXXX Mason Dale Drive, email address of okellochatrie55@gmail.com, and phone number of 804-475-8298 during the course of his employment with the home improvement store.

Pursuant to the GeoFence warrant, law enforcement then requested and obtained subscriber information for the Chatrie Account, and two additional anonymized accounts. On July 11, 2019, Google provided subscriber information for just these three accounts. The United States did not obtain any subscriber or other identifying information on the other 16 anonymized accounts. The subscriber information for the Chatrie Account had the email of okellochatrie55@gmail.com, a name of "Jamaican media," and showed a last login date of May 20, 2019, the date of the robbery of Call Federal Credit Union.

Law enforcement later obtained a federal search warrant on July 17, 2019, for historical location information for the Google account of okellochatrie55@gmail.com and Google account ID: 365520819283.[4] That location information demonstrated, among other things, that the account left XXXX Mason Dale Drive before the robbery and returned to XXXX Mason Dale Drive after the robbery.

Law enforcement also sought and obtained a federal search warrant on July 17, 2019, for historical and prospective location information from Sprint Mobile for the cellular telephone

[4] Importantly, the historical information obtained for Chatrie's account is the same type of information gleaned from the GeoFence warrant. That is, location information for Chatrie's Google account.

number 804-475-8298. It was later determined that the Sprint account for this phone number was deactivated on July 7, 2019.

On July 19, 2019, law enforcement sought and obtained federal search warrants, one for a cell site simulator to ascertain the defendant's new phone number[5] and another to place a tracking device on the defendant's 2010 blue Buick Lacrosse. At the same time, law enforcement obtained and analyzed toll records from Sprint for the defendant's phone, his father's phone, and his sister's phone. Analysis of the defendant's father's and sister's toll records revealed a telephone number in common that was later discovered to belong to the defendant, despite having someone else listed as the subscriber for the T-Mobile telephone.

Law enforcement also surveilled the defendant beginning in mid-July. Surveillance of the defendant and his vehicle revealed that he spent the vast majority of his time at XXXX Willis Street and XXX Rosegill Road.

Further review of the historical location information obtained from the federal search warrant obtained on July 17, 2019, showed that the defendant spent much of his time at XXXX Mason Dale Drive during the week prior to the robbery, was near the Call Federal Credit Union at the time of the robbery, was near XXXX Mason Dale Drive before and after the robbery, and spent several hours at XXX Rosegill Road. During the week following the armed robbery, the defendant's phone was located at XXXX Mason Dale Drive and the Rosegill residence. Law enforcement surveillance between July 23, 2019, and August 12, 2019, revealed that the defendant spent most of his evenings at XXXX Willis Street.

On August 12, 2019, law enforcement sought and obtained a search warrant for the

[5] No evidence of value was obtained from the use of the cell site simulator.

residences located at XXXX Mason Dale Drive, XXXX Willis Street, XXX Rosegill Road, and the Buick Lacrosse. When executing these search warrants in the early morning of August 13, 2019, law enforcement recovered evidence of value from XXXX Mason Dale Drive and XXXX Willis Street. At the XXXX Mason Dale Drive residence, law enforcement recovered two robbery-style demand notes from the bedroom belonging to the defendant. At XXXX Willis Street, law enforcement recovered nearly $100,000 in United States Currency (including bills wrapped in bands signed by the victim-bank teller), a silver and black firearm that appeared to be identical to the firearm used in the robbery, a money counter, and a safe.[6]

The defendant was at XXXX Willis Street when the search warrant was executed. After being placed under arrest and advised of his *Miranda* rights, the defendant admitted to the armed robbery of the Call Federal Credit Union on May 20, 2019.

On September 17, 2019, a Richmond grand jury returned a two-count indictment for Forced Accompaniment during an Armed Credit Union Robbery, in violation of 18 U.S.C. § 2113(e), and Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A)(i). The defendant pleaded not guilty on October 1, 2019, and trial was scheduled for December 3, 2019, through December 5, 2019, at 9:00 a.m. before the Honorable M. Hannah Lauck. At a status conference, on November 12, 2019, the Court granted the defendant's motion to continue trial beyond the speedy trial date. (ECF No. 34)

On October 22, 2019, the defendant filed the Motions to Suppress that are subject of this response.

[6] All electronics recovered—whether cellular telephones or computers—returned no evidence of value. Moreover, the defendant and his girlfriend provided consent to search the cellular telephones and computers recovered from XXXX Willis Street.

II. ARGUMENT

A. The Search Warrant had Sufficient Particularity

The defendant contends that the warrant is overbroad because it permits law enforcement to "obtain all activity logs, security questions and answers, passwords, posts, and all other 'Google Activities." Def.'s Mot. to Suppress, ECF No. 20 at 2-3. The defendant then points to Section II. of Attachment B, which permits the United States to seize, from the evidence disclosed by Google, "[e]vidence indicating how and when the Google account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Google account owner." 3:19-SW-207 at 15.

The defendant's baseline contention—that the warrant permits for an expansive, indiscriminate search of all electronic data—is simply wrong. In this case, the warrants' descriptions of the items subject to seizure were adequately particularized because they identified the items to be seized by their relation to designated crimes, and in so doing, adequately limited the executing agents' discretion. *See United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017) (Gorsuch, J.) ("[W]arrants may pass the particularity test if they limit their scope either to evidence of specific federal crimes or to specific types of material.") (internal citations and quotations omitted). Specifically, Attachment B to the Google Account warrant authorized agents to seize only information relating to the robbery of any commercial business or a conspiracy to do so, or to "records and information relating to" any of the subject offenses. 3:19-SW-207 at 15. Accordingly, the executing agents were authorized "to seize only evidence of a particular crime" and could not engage in exploratory searches for general evidence of criminality. *See United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986); *See also United States v. Anthony*, 4 F.3d

986, 1993 WL 321595, at *2 (4th Cir. Aug. 24, 1993) (unpublished table decision) (upholding warrant that authorized agents to search for evidence relating to the crime of bank robbery because it sufficiently "provide[d] that degree of specificity required by the precedent of this court.").

That the search of the defendant's data necessarily involved a cursory review of innocuous items does not render the warrant constitutionally defective. *See United States v. Williams*, 592 F.3d 511, 520–21 (4th Cir. 2010) ("When a search requires review of a large collection of items, such as papers, 'it is certain that some innocuous documents will be examined, at least cursorily, in order to deter mine whether they are, in fact, among those papers authorized to be seized.'").

Additionally, the defendant's argument that the Google account warrant is lacking in particularity misunderstands the nature of electronic evidence, and the reasonable means necessary to examine it in order to locate and extract the files that contain the evidence allowed to be seized pursuant to a search warrant. Attachment B, Section I itemized all the information to be disclosed by Google in connection with the identified Google accounts. For example, the warrant required Google to disclose "all activity logs for the account and all other documents showing the user's posts and other Google Activities." However, Attachment B, Section II then identified the information to be seized from what Google produced. That information centered around the armed robbery of the Call Federal Credit Union.

Despite the clear particularity of the warrant and accompanying documents in this case, the defendant calls the Court's attention to case law that is wholly inapposite.

Consider, for example, *Coolidge v. New Hampshire*. 403 U.S. 443 (1971). There, the Supreme Court analyzed the warrantless search and seizure of a defendant's car after concluding that the warrant issued for that automobile was not issued by "neutral and detached magistrate." *Id.* at 453. In that context, the Supreme Court rejected the government's contention that the plain

view doctrine nevertheless protected the search of the automobile by pointing to the underpinnings of the warrant requirement. In doing so, the *Coolidge* Court pointed, in part, to the interest in having searches be "as limited as possible" to avoid subjection to an "exploratory rummaging" of [one's] "belongings." *Id.* at 467. That was the extent of the Supreme Court's particularity analysis in *Coolidge*. One of the cases cited in *Coolidge* for the aforementioned proposition is also cited by the defendant. Like *Coolidge*, *Stanford v. Texas* does nothing to redeem the defendant's argument. 379 U.S. 476 (1965).

In *Stanford*, the Supreme Court dealt with the interplay between the First and Fourth Amendment, reminding that the Fourth Amendment guards against more than writs of assistance permitting general searches whenever and wherever. *Id.* at 482. Rather, the *Stanford* Court noted, the protection of freedom of expression through literature and the like was sacrosanct to a robust Fourth Amendment protection. *Id.* ("[T]hings to be seized" must "be accorded the most scrupulous exactitude when the things are books, and the basis for their seizure is the ideas which they contain."). Indeed, the Supreme Court eschewed analogizing to seizure of "weapons, narcotics or cases of whiskey" because rather than contraband of any kind the warrant at issue in *Stanford* permitted seizure of "literary material" concerning the Community Party of Texas and operations of that party. *Id.* at 486. This "language," the Court opined, was "constitutionally intolerable" as it swept too broadly. Stated simply, the defendant's reliance on these cases is misplaced, because he takes their language out of its context.

The two Fourth Circuit decisions cited by the defendant are similarly unavailing. In addition to *Fawole*, the defendant mentions *United States v. Uzenski*. 434 F.3d 690 (4th Cir. 2006).

In *Uzenski*, a panel assessed whether blanket suppression should result from law enforcement seizing items outside the scope of a residential search warrant during a search for

evidence relating to a defendant's manufacture of home-made pipe bombs. In analyzing that issue, the panel explained that blanket suppression is an "extraordinary remedy" reserved for extreme circumstances and is not a remedy "[e]ven where officers exceed the bounds of their authority pursuant to the warrant . . . [and] seize[] items [ ] not identified in the warrant." *Id.* at 706. The *Uzenski* panel made plain that blanket suppression is only warranted where "a fishing expedition for the discovery of incriminating evidence" occurs—for example, where a warrant authorizes search for four weapons and marijuana but the searching agencies seize thirty-five items, including firearms, ammunition, and various drug paraphernalia or where officers seized 667 items not specified by the warrant. *Id.* In this case, the officers seized only that information that they were authorized to seize by the warrant, rendering *Uzenski* wholly irrelevant.

In short, the Google Account warrant in this matter sought with sufficient particularity evidence that defendant committed the armed robbery of the Call Federal Credit Union on May 20, 2019.

B. The Search Warrant had Sufficient Nexus between the Defendant's Cellular Telephone and the $200,000 Armed Robbery of the Call Federal Credit Union

The defendant argues that the search warrant for the defendant's Google Account was not supported by probable cause—that is, probable cause that evidence of the crime, save for location information, would be contained within the Google accounts. Def.'s Mot. to Suppress at 4-6. As the defendant does in other motions, he cites to inapplicable narcotics cases to support his misguided contention.

Probable cause is a "practical, nontechnical conception," and a magistrate judge's determination of this practical conception is "to be paid great deference by reviewing courts" so as to avoid the "after-the-fact scrutiny by courts of the sufficiency of an affidavit . . . tak[ing] the form of de novo review." *United States v. Graham*, 93 F. App'x 511, 514 (4th Cir. 2004)

(unpublished) (per curiam). "[The] inquiry is thus limited to whether there was a substantial basis for determining the existence of probable cause." *See United States v. McNeal*, 818 F.3d 141, 154–55 (4th Cir. 2016). Probable cause requires only "a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)).

The defendant's argument on this front begins with the contention that law enforcement provided no specific information about why officers would find any evidence of the alleged crime, other than location data, on the Google accounts. That assertion is baseless. Paragraph 30 of the affidavit provides:

> Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

Further elaborating upon the presence of more than mere location information, paragraph 36 provides that "information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email)." Accordingly, the affidavit states that, "the servers of Google are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Google, such as account access information, transaction information, and other account information." Lastly, the affidavit provides the relevance of the sought after information from Google:

> information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

The information gleaned from this Google account warrant would plausibly serve various purposes in the investigation and prosecution of the armed robbery, including tying the defendant to the account and authenticating his use of the Google account. *See* United States District Judge Paul Grimm (D. Md.), *Best Practices for Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1, (2017). For example, in connecting the defendant with the Chatrie Account—a critically important piece of evidence—the United States could rely upon posts connected to his various Google Activities, such as "check ins," that reveal "nonpublic details o[his] life," "references or links to, or contact information about, loved ones, relatives, co-workers, [and] others close to the purported author," and "photos and videos likely to be accessed by the purported author." *Id.* at 20; *see also Messerschmidt v. Millender*, 565 U.S. 535, 552 n.7 (2012) ("The Fourth Amendment does not require probable cause to believe evidence will conclusively establish a fact before permitting a search, but only 'probable cause . . . to believe that the evidence sought *will aid* in a particular apprehension or conviction.'") (alteration in original).

The defendant then goes on to argue that there was no probable cause that his Google account was used at all because there is no witness identifying him using "his Google accounts in planning or executing a robbery" and no witness of his use of any Google account during the robbery. Def.'s Mot. to Suppress at 4. Again, this argument is premised on the incorrect notion that there must be direct evidence linking the items sought to the defendant's Google Account. *See, e.g.*, *United States v. Wienke*, 733 F. App'x 65, 69 (4th Cir. 2018) (unpublished) (per curiam) (holding that a "magistrate may draw a reasonable inference from the facts stated if the affiant

does not assert facts 'directly linking the items sought to the defendant's residence.'").

The defendant's argument also disregards the affidavit's explanation that cellular telephones are used by coconspirators to "communicate with each other via voice calls, text messages, and emails, and the internet, permitting them to plan, coordinate, and execute their crimes" and "people often take pictures utilizing their cellular telephones that may implicate them in a crime, i.e., possessing a firearm, posing with large quantities stolen items, or large amounts of cash." Moreover, the search warrant came on the heels of the discovery that a Google account with subscriber information that included the email of okellochatrie55@gmail.com fit the description of the armed robbery.

The defendant does not contest that there is probable cause that he committed the armed robbery at the Call Federal Credit Union. He similarly does not contest the fact that video of the armed robber shows the armed robber with a cellular telephone next to his face when he entered the Credit Union. The issuing magistrate had a substantial basis for finding probable cause for information associated with the Defendant's Google Account.

The cases cited by the defendant to combat probable cause for these items do little to provide meaningful analysis here. To begin, the Fourth Circuit's decision in *United States v. Lyles* concerned an affidavit premised on a single trash pull resulting in the discovery of three marijuana stems. 910 F.3d 787, 794 (4th Cir. 2018). This trash pull, standing alone, did not support probable cause to search the residence for marijuana possession. *Id.* The case has no analytical value in this case and on these facts. No different with the district court decision out of Kentucky. *See United States v. Ramirez*, 180 F. Supp. 3d 491 (W.D. Ky. 2016). *Ramirez* concerns an equally skeletal affidavit relying specifically upon the arrest of the defendant for a conspiracy to distribute narcotics arrest and the presence of the cell phone during the defendant's arrest:

> The four corners of affidavit assert the following facts: 1) when Detective Petter arrested Ramirez on May 16, 2013, for conspiring to possess marijuana with the intent to distribute, he "was in possession of a Verizon Motorola cell phone, blue and gray in color, with phone number (502) 552-7460," and the cell phone was seized; 2) Detective Petter knew "through training and field experience that individuals may keep text messages or other electronic information stored in their cell phones which may relate them to the crime and/or co-defendants/victim." Aff. 1–2.

Id. at 494.

The affidavit failed to provide any details of the arrest or charges, investigatory steps taken, such as wiretap warrants, evidence obtained in the search of the defendant's residence, or the fact of an ongoing DEA investigation. *Id.* at 496.

In sharp contrast, here, the affidavits provided numerous details about the investigation, and evidence linking the defendant to the crime, and establishing a fair probability that the Google Account would contain relevant evidence. Furthermore, the affidavit in this case points out that the defendant was actually using his cell phone at the credit union. Accordingly, the defendant cannot carry his burden that the warrant's authorization to search and seize location information from his Google Account was not supported by probable cause.

C. Suppression would be Unwarranted under United States v. Leon's Good-Faith Exception

Even if defendant's particularity and probable cause challenge were deemed meritorious, suppression would be unwarranted under the good-faith exception to the exclusionary rule. *See United States v. Leon*, 468 U.S. 897, 922 (1984); *see also United States v. Burton*, 756 Fed. Appx 295, 300-01 (4th Cir. 2018) (assuming, without deciding that cell phone and home warrants were overbroad, court found that officers acted in good-faith reliance on warrants); *United States v. Qazah*, 810 F.3d 879, 885-86 (4th Cir. 2015) (explaining that "[w]hen officers obtain a search warrant but the requirements of the Fourth Amendment are nonetheless violated, evidence

recovered during the search may" be excluded "in certain egregious cases," but that "in the ordinary course, the exclusion of evidence is not the proper remedy"), *cert. denied*, 136 S. Ct. 2398 (2016).

According to *Leon*, "the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates. 468 U.S. at 898. As such, exclusion is not an available remedy when the law enforcement officers executing a warrant follow its instructions. As the Supreme Court has explained, the exclusionary rule "does not apply when the police conduct a search in 'objectively reasonable reliance' on a warrant later held invalid." *Davis v. United States*, 564 U.S. 229, 238-39 (2011) (quoting *Leon*, 468 U.S. at 922). "The error in such a case rests with the issuing magistrate, not the police officer, and 'punish[ing] the errors of judges' is not the office of the exclusionary rule." *Id.* at 239 (quoting *Leon*, 468 U.S. at 916). Of relevance here, the Court has applied that reasoning both where the warrant was allegedly unsupported by probable cause (as in *Leon*, 468 U.S. at 903), and where it was found to be overbroad (as in the companion case of *Massachusetts v. Sheppard*, 468 U.S. 981, 988–91 (1984)).

The circumstances of this case fall within the heartland of the good-faith exception. The Affiant prepared a substantive, detailed affidavit that: (a) described facts that undisputedly establish probable cause to believe that defendant committed the subject offenses; and (b) also included facts that led a neutral magistrate to find probable cause that evidence of those violations would be found in the defendant's Google Account. The warrant applications were reviewed by prosecutors. The Affiant then submitted the applications to a magistrate judge. Having thus taken "every step that could reasonably be expected," the Affiant was entitled to conclude "that the warrant[s] authorized a search for the materials outlined in the affidavit[s]," *Sheppard*, 468 U.S. at 989. *See United States v. McLamb*, 880 F.3d 685, 690-91 (4th Cir. 2018) (good-faith exception

applied where no "judicial precedent" had re-solved legal questions underlying the issuing judge's authority and the FBI consulted with prosecutors before seeking the warrant).

None of the exceptions recognized in *Leon* apply here. *See United States v. Wellman*, 663 F.3d 224, 228–29 (4th Cir. 2011). Even if the affidavit ultimately is deemed to lack sufficient particularity or fails to provide a nexus between the Google accounts and the armed robbery, it was not so "bare bones" or "so lacking in indicia of probable cause" as to render "official belief in its existence was objectively unreasonable." In this case, nothing in the record suggests that any of these situations applies, and defendant has made no claim to the contrary.

III. CONCLUSION

The Court should deny the defendant's motions to suppress evidence obtained from his Google Account.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 19th day of November, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov